#2 E-Werner 3-16-01

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

jc860 U.S. PTO 09/748176 12/27/00

In re Application of:	
Yutaka ICHINOI et al.	
Serial No.	Art Unit:
Filed: December 27, 2000	Examiner:
For: CONTENTS-INFORMATION TRANSMISSION SYSTEM	Atty Docket: 0102/0154

SUBMISSION OF PRIORITY DOCUMENTS

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Attached hereto please find a certified copies of applicants' Japanese applications as follows:

Japanese Patent Application No. 2000-79112 filed February 14, 2000
Japanese Patent Application No. 2000-57785 filed March 2, 2000

Applicants request the benefit of said February 14, 2000 filing date for priority purposes pursuant to the provisions of 35 USC 119.

Respectfully submitted,

Louis Woo, RN 31,730
Law Offices of Louis Woo
1901 North Fort Myer Drive, Suite 501
Arlington, VA 22209
(703) 522-8872

Date: Dec 27 2000

U4-0026-TH (1)

JC860 U.S. PTO 09/748176 12/27/00

日　本　国　特　許　庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出願年月日 Date of Application:	２０００年　２月１４日
出願番号 Application Number:	特願２０００－０７９１１２
出願人 Applicant (s):	日本ビクター株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年１２月１５日

特許庁長官
Commissioner,
Patent Office

及川耕造

出証番号　出証特２０００－３１０４４２３

【書類名】　特許願
【整理番号】　412000083
【あて先】　特許庁長官殿
【国際特許分類】　G06F 19/00
【発明者】
　【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内
　【氏名】　一井　豊
【発明者】
　【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内
　【氏名】　大石　剛士
【特許出願人】
　【識別番号】　000004329
　【氏名又は名称】　日本ビクター株式会社
【代理人】
　【識別番号】　100093067
　【弁理士】
　【氏名又は名称】　二瓶　正敬
【手数料の表示】
　【予納台帳番号】　039103
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9004770

【書類名】　明細書
【発明の名称】　コンテンツ伝送システム、認証機器、コンテンツ取扱装置、データ伝送方法、記録媒体、伝送媒体、信頼度判定装置、信頼度被判定装置、信頼度判定システム、信頼度判定方法、信頼度被判定方法、情報送信装置、情報伝送方法
【特許請求の範囲】
【請求項１】　複数の異なる著作権保護レベル及び／又は守秘能力の１つを有するコンテンツ取扱装置と、前記コンテンツ取扱装置に対して伝送媒体を介して接続可能であり、前記コンテンツ取扱装置が所定の著作権保護レベル及び／又は守秘能力を有しているか否かを判断してコンテンツを前記コンテンツ取扱装置に送信する認証機器とを有するコンテンツ伝送システムであって、
認証のための所定データが前記認証機器から前記コンテンツ取扱装置に送信され、前記コンテンツ取扱装置が受信した前記所定データに基づいて自身の著作権保護レベル及び／又は守秘能力を示すデータが前記コンテンツ取扱装置から前記認証機器に送信され、前記著作権保護レベル及び／又は守秘能力を示すデータが前記認証機器においてあらかじめ設定した基準レベルと比較され、比較結果に応じてコンテンツを前記認証機器から前記コンテンツ取扱装置に送信するか否かの制御が行われるよう構成されたコンテンツ伝送システム。
【請求項２】　複数の異なる著作権保護レベル及び／又は守秘能力の１つを有するコンテンツ取扱装置に対して伝送媒体を介して接続可能であり、前記コンテンツ取扱装置が所定の著作権保護レベル及び／又は守秘能力を有しているか否かを判断してコンテンツを前記コンテンツ取扱装置に送信する認証機器であって、
認証のための所定データを前記コンテンツ取扱装置に送信する手段と、前記コンテンツ取扱装置が前記所定のデータに基づいて自身の著作権保護レベル及び／又は守秘能力を示すデータを作成して前記認証機器に送信したとき、これを受信する手段と、前記著作権保護レベル及び／又は守秘能力を示すデータとあらかじめ設定した基準レベルとを比較する手段と、比較結果に応じてコンテンツを前記コンテンツ取扱装置に送信するか否かの制御を行う制御手段とを、

有する認証機器。

【請求項３】　複数の異なる著作権保護レベル及び／又は守秘能力の１つを有するコンテンツ取扱装置と、前記コンテンツ取扱装置に対して伝送媒体を介して接続可能であり、前記コンテンツ取扱装置が所定の著作権保護レベル及び／又は守秘能力を有しているか否かを判断してコンテンツを前記コンテンツ取扱装置に送信する認証機器とを有するコンテンツ伝送システムにおける前記コンテンツ取扱装置であって、

認証のための所定データが前記認証機器から前記コンテンツ取扱装置に送信されたとき、受信した前記所定データに基づいて自身の著作権保護レベル及び／又は守秘能力を示すデータを前記認証機器に送信する手段を有するコンテンツ取扱装置。

【請求項４】　複数の異なる著作権保護レベル及び／又は守秘能力の１つを有するコンテンツ取扱装置と、前記コンテンツ取扱装置に対して伝送媒体を介して接続可能であり、前記コンテンツ取扱装置が所定の著作権保護レベル及び／又は守秘能力を有しているか否かを判断してコンテンツを前記コンテンツ取扱装置に送信する認証機器とを有するコンテンツ伝送システム用におけるデータ伝送方法であって、

認証のための前記所定データを前記認証機器から前記コンテンツ取扱装置に送信するステップと、

前記コンテンツ取扱装置が受信した前記所定データに基づいて自身の著作権保護レベル及び／又は守秘能力を示すデータを前記コンテンツ取扱装置から前記認証機器に送信するステップと、

前記著作権保護レベル及び／又は守秘能力を示すデータが前記認証機器においてあらかじめ設定した基準レベルと比較され、比較結果に応じて前記認証機器から前記コンテンツ取扱装置にコンテンツを送信するよう制御するステップとを、

有するデータ伝送方法。

【請求項５】　複数の異なる著作権保護レベル及び／又は守秘能力の１つを有するコンテンツ取扱装置と、前記コンテンツ取扱装置に対して伝送媒体を介して接続可能であり、前記コンテンツ取扱装置が所定の著作権保護レベル及び／又

は守秘能力を有しているか否かを判断してコンテンツを前記コンテンツ取扱装置に送信する認証機器とを有するコンテンツ伝送システム用の前記伝送媒体であって、

認証のための前記所定データを前記認証機器から前記コンテンツ取扱装置に送信し、前記コンテンツ取扱装置が受信した前記所定データに基づいて自身の著作権保護レベル及び／又は守秘能力を示すデータを前記コンテンツ取扱装置から前記認証機器に送信し、前記著作権保護レベル及び／又は守秘能力を示すデータが前記認証機器においてあらかじめ設定した基準レベルと比較され、比較結果に応じて前記認証機器から前記コンテンツ取扱装置にコンテンツを送信するための伝送媒体。

【請求項６】　著作権保護及び／又は守秘能力を有するコンテンツ取扱装置と、前記コンテンツ取扱装置に対して伝送媒体を介して接続可能であり、前記コンテンツ取扱装置が前記著作権保護及び／又は守秘能力を有しているか否かを判断してコンテンツを前記コンテンツ取扱装置に送信する認証機器とを有するコンテンツ伝送システムであって、

認証のための所定データが前記認証機器から前記コンテンツ取扱装置に送信され、前記コンテンツ取扱装置が受信した前記所定データに基づいて自身の著作権保護及び／又は守秘能力を示すデータとして著作権の存在するコンテンツを含むデータが前記コンテンツ取扱装置から前記認証機器に送信され、前記著作権保護及び／又は守秘能力を示すデータが前記認証機器において認識され、認識結果に応じてコンテンツを前記認証機器から前記コンテンツ取扱装置に送信するか否かの制御が行われるよう構成されたコンテンツ伝送システム。

【請求項７】　著作権保護及び／又は守秘能力を有するコンテンツ取扱装置に対して伝送媒体を介して接続可能であり、前記コンテンツ取扱装置が前記著作権保護及び／又は守秘能力を有しているか否かを判断してコンテンツを前記コンテンツ取扱装置に送信する認証機器であって、

認証のための所定データを前記コンテンツ取扱装置に送信する手段と、前記コンテンツ取扱装置が前記所定のデータに基づいて自身の著作権保護及び／又は守秘能力を示すデータとして著作権の存在するコンテンツを含むデータを作成して

前記認証機器に送信したとき、これを受信する手段と、前記著作権保護及び／又は守秘能力を示すデータを認識する手段と、認識結果に応じてコンテンツを前記コンテンツ取扱装置に送信するか否かの制御を行う制御手段とを、

有する認証機器。

【請求項８】　著作権保護及び／又は守秘能力を有するコンテンツ取扱装置と、前記コンテンツ取扱装置に対して伝送媒体を介して接続可能であり、前記コンテンツ取扱装置が前記著作権保護及び／又は守秘能力を有しているか否かを判断してコンテンツを前記コンテンツ取扱装置に送信する認証機器とを有するコンテンツ伝送システムにおける前記コンテンツ取扱装置であって、

認証のための所定データが前記認証機器から前記コンテンツ取扱装置に送信されたとき、受信した前記所定データに基づいて自身の著作権保護及び／又は守秘能力を示すデータとして著作権の存在するコンテンツを含むデータを前記認証機器に送信する手段を有するコンテンツ取扱装置。

【請求項９】　著作権保護及び／又は守秘能力を有するコンテンツ取扱装置と、前記コンテンツ取扱装置に対して伝送媒体を介して接続可能であり、前記コンテンツ取扱装置が前記著作権保護及び／又は守秘能力を有しているか否かを判断してコンテンツを前記コンテンツ取扱装置に送信する認証機器とを有するコンテンツ伝送システム用におけるデータ伝送方法であって、

認証のための前記所定データを前記認証機器から前記コンテンツ取扱装置に送信するステップと、

前記コンテンツ取扱装置が受信した前記所定データに基づいて自身の著作権保護及び／又は守秘能力を示すデータとして著作権の存在するコンテンツを含むデータを前記コンテンツ取扱装置から前記認証機器に送信するステップと、

前記著作権保護及び／又は守秘能力を示すデータが前記認証機器において認識され、認識結果に応じて前記認証機器から前記コンテンツ取扱装置にコンテンツを送信するよう制御するステップとを、

有するデータ伝送方法。

【請求項１０】　著作権保護及び／又は守秘能力を有するコンテンツ取扱装置と、前記コンテンツ取扱装置に対して伝送媒体を介して接続可能であり、前記

コンテンツ取扱装置が前記著作権保護及び／又は守秘能力を有しているか否かを判断してコンテンツを前記コンテンツ取扱装置に送信する認証機器とを有するコンテンツ伝送システム用の前記伝送媒体であって、

認証のための前記所定データを前記認証機器から前記コンテンツ取扱装置に送信し、前記コンテンツ取扱装置が受信した前記所定データに基づいて自身の著作権保護及び／又は守秘能力を示すデータとして著作権の存在するコンテンツを含むデータを前記コンテンツ取扱装置から前記認証機器に送信し、前記著作権保護及び／又は守秘能力を示すデータが前記認証機器において認識され、認識結果に応じて前記認証機器から前記コンテンツ取扱装置にコンテンツを送信するための伝送媒体。

【請求項１１】　情報の守秘能力に応じてあらかじめ複数の信頼度に分類されている対象装置の信頼度を判定する信頼度判定装置であって、

前記所定のデータを前記対象装置に送る送信手段と、

前記所定のデータを送った返答として前記対象装置から送られるデータを受け取る受信手段と、

前記複数の信頼度の全てに対応した複数の公開鍵が記憶されている記憶手段と、

前記複数の公開鍵のいずれかを用いて前記対象装置から送られるデータを解読する解読手段と、

前記所定のデータと前記解読手段により解読されたデータとが一致しているかどうか判断する判断手段と、

前記判断手段における判断において前記解読されたデータと前記所定のデータとが一致した場合、前記解読手段で用いられた公開鍵に対応した信頼度が前記対象装置の信頼度であると判定する判定手段とを、

有する信頼度判定装置。

【請求項１２】　情報の守秘能力に応じてあらかじめ複数の信頼度に分類されている装置の信頼度を判定する信頼度判定装置により信頼度を判定される信頼度被判定装置であって、

前記信頼度判定装置から送られる所定のデータを受け取る受信手段と、

前記複数の信頼度の特定の１つに対応した秘密鍵が記憶されている記憶手段と、

前記秘密鍵を用いて前記所定のデータを暗号化する暗号化手段と、

前記暗号化手段で暗号化されたデータを前記信頼度判定装置に送る送信手段とを、

有する信頼度被判定装置。

【請求項１３】　情報の守秘能力に応じてあらかじめ複数の信頼度に分類されている装置の信頼度を判定する信頼度判定装置と、

前記信頼度判定装置により信頼度を判定される信頼度被判定装置とを有する信頼度判定システムであって、

前記信頼度判定装置は、

前記所定のデータを前記信頼度被判定装置に送る送信手段と、

前記所定のデータを送った返答として前記信頼度被判定装置から送られるデータを受け取る受信手段と、

前記複数の信頼度の全てに対応した複数の公開鍵が記憶されている記憶手段と、

前記複数の公開鍵のいずれかを用いて前記信頼度被判定装置から送られるデータを解読する解読手段と、

前記所定のデータと前記解読手段により解読されたデータとが一致しているかどうか判断する判断手段と、

前記判断手段における判断において前記解読されたデータと前記所定のデータとが一致した場合、前記解読手段で用いられた公開鍵に対応した信頼度が前記信頼度被判定装置の信頼度であると判定する判定手段とを有し、

前記信頼度被判定装置は、

前記信頼度判定装置から送られる所定のデータを受け取る受信手段と、

前記複数の信頼度の特定の１つに対応した秘密鍵が記憶されている記憶手段と、

前記秘密鍵を用いて前記所定のデータを暗号化する暗号化手段と、

前記暗号化手段で暗号化されたデータを前記信頼度判定装置に送る送信手段

とを、

有する信頼度判定システム。

【請求項１４】　信頼度判定装置側から信頼度被判定装置側へコンテンツの伝送を行うためのもので、情報の守秘能力に応じて前記信頼度被判定装置側はあらかじめ複数の信頼度に分類されており、前記信頼度被判定装置側には前記信頼度に対応した秘密鍵が記憶されており、前記信頼度判定装置側には全ての前記複数の信頼度の全てに対応した複数の公開鍵が記憶されている信頼度判定方法であって、

前記信頼度判定装置側において、前記信頼度被判定装置側に対して所定のデータを送るステップと、

前記信頼度判定装置側において、前記所定のデータを送った返答として、前記信頼度被判定装置で前記暗号化されたデータを受け取るステップと、

前記信頼度判定装置側において、前記複数の公開鍵を用いて、前記暗号化されたデータを解読するステップと、

前記信頼度判定装置側において、前記解読されたデータと前記信頼度判定装置側があらかじめ有する所定のデータとが一致しているかどうか判断するステップと、

前記判断するステップにおいて、前記解読されたデータと前記所定のデータとが一致した場合、前記解読されたデータの解読に用いた公開鍵に対応した信頼度が前記信頼度被判定装置側の信頼度であると判定するステップとを有する信頼度判定方法。

【請求項１５】　信頼度判定装置側から信頼度被判定装置側へコンテンツの伝送を行うためのもので、情報の守秘能力に応じて前記信頼度被判定装置側はあらかじめ複数の信頼度に分類されており、前記信頼度被判定装置側には前記信頼度に対応した秘密鍵が記憶されており、前記信頼度判定装置側には全ての前記複数の信頼度の全てに対応した複数の公開鍵が記憶されている信頼度被判定方法であって、

前記信頼度被判定装置側において、前記信頼度判定装置側から所定のデータを受け取るステップと、

前記信頼度被判定装置側において、前記秘密鍵を用いて、前記所定のデータを暗号化するステップと、

前記信頼度被判定装置側において、前記信頼度判定装置側に対して前記暗号化するステップで暗号化されたデータを送るステップとを、

有する信頼度被判定方法。

【請求項１６】　信頼度判定装置側から信頼度被判定装置側へコンテンツの伝送を行うためのもので、情報の守秘能力に応じて前記信頼度被判定装置側はあらかじめ複数の信頼度に分類されており、前記信頼度被判定装置側には前記信頼度に対応した秘密鍵が記憶されており、前記信頼度判定装置側には全ての前記複数の信頼度の全てに対応した複数の公開鍵が記憶されている信頼度判定方法を実行するためのプログラムが記録された記録媒体であって、

前記信頼度判定装置側において、前記信頼度被判定装置側に対して所定のデータを送るステップと、

前記信頼度判定装置側において、前記所定のデータを送った返答として、前記信頼度被判定装置で前記秘密鍵により暗号化されたデータを受け取るステップと、

前記信頼度判定装置側において、前記複数の公開鍵のいずれかを用いて、前記暗号化されたデータを解読するステップと、

前記信頼度判定装置側において、前記解読されたデータと前記信頼度判定装置側があらかじめ有する所定のデータとが一致しているかどうか判断するステップと、

前記判断するステップにおいて、前記解読されたデータと前記所定のデータとが一致した場合、前記解読されたデータの解読に用いた公開鍵に対応した信頼度が前記信頼度被判定装置側の信頼度であると判定するステップとを有する信頼度判定方法を実行するためのプログラムが記録された記録媒体。

【請求項１７】　信頼度判定装置側から信頼度被判定装置側へコンテンツの伝送を行うためのもので、情報の守秘能力に応じて前記信頼度被判定装置側はあらかじめ複数の信頼度に分類されており、前記信頼度被判定装置側には前記信頼度に対応した秘密鍵が記憶されており、前記信頼度判定装置側には全ての前記複

数の信頼度の全てに対応した複数の公開鍵が記憶されている信頼度被判定方法を実行するためのプログラムが記録された記録媒体であって、

前記信頼度被判定装置側において、前記信頼度判定装置側から所定のデータを受け取るステップと、

前記信頼度被判定装置側において、前記秘密鍵を用いて、前記所定のデータを暗号化するステップと、

前記信頼度被判定装置側において、前記信頼度判定装置側に対して前記暗号化するステップで暗号化されたデータを送るステップとを、

有する信頼度被判定方法を実行するためのプログラムが記録された記録媒体。

【請求項１８】　情報の守秘能力に応じてあらかじめ複数の信頼度に分類されている情報受信装置にコンテンツの伝送を行うための情報送信装置であって、

所定のデータが記憶されている第１の記憶手段と、

前記所定のデータを前記情報受信装置に送る第１の送信手段と、

前記所定のデータを送った返答として前記情報受信装置から送られるデータを受け取る受信手段と、

前記複数の信頼度の全てに対応した複数の公開鍵が記憶されている第２の記憶手段と、

前記複数の公開鍵のいずれかを用いて前記情報受信装置から送られるデータを解読する解読手段と、

前記所定のデータと前記解読手段により解読されたデータとが一致しているかどうか判断する判断手段と、

前記判断手段における判断において前記解読されたデータと前記所定のデータとが一致した場合、前記解読手段で用いられた前記公開鍵に対応した信頼度が前記情報受信装置の信頼度であると判定する判定手段と、

前記判定手段により判定された前記情報受信装置の信頼度に応じて、前記情報受信手段への前記コンテンツの送信を制御する制御手段と、

前記制御手段の制御の下で、前記コンテンツを前記情報受信手段に送信する第２の送信手段とを、

有する情報送信装置。

【請求項１９】　情報送信装置から情報受信装置へコンテンツの伝送を行うためのもので、情報の守秘能力に応じて前記情報受信装置はあらかじめ複数の信頼度に分類されており、前記情報受信装置には前記複数の信頼度の特定の１つに対応した秘密鍵が記憶されており、前記情報送信装置には全ての前記複数の信頼度の全てに対応した複数の公開鍵が記憶されている情報伝送方法であって、

前記情報送信装置において、前記情報受信装置に対して所定のデータを送るステップと、

前記情報送信装置において、前記所定のデータを送った返答として、前記情報受信装置で前記秘密鍵により暗号化されたデータを受け取るステップと、

前記情報送信装置において、前記複数の公開鍵のいずれかを用いて、前記暗号化されたデータを解読するステップと、

前記情報送信装置において、前記解読されたデータと前記所定のデータとが一致しているかどうか判断するステップと、

前記判断するステップにおいて、前記解読されたデータと前記所定のデータとが一致した場合、前記解読手段で用いられた公開鍵に対応した信頼度が前記情報受信装置の信頼度であると判定するステップと、

前記判定された前記情報受信装置の信頼度に応じて制御しながら、前記情報送信装置から前記情報受信装置へ前記コンテンツを送るステップとを、

有する情報伝送方法。

【請求項２０】

情報送信装置から情報受信装置へコンテンツの伝送を行うためのもので、情報の守秘能力に応じて前記情報受信装置はあらかじめ複数の信頼度に分類されており、前記情報受信装置には前記複数の信頼度の特定の１つに対応した秘密鍵が記憶されており、前記情報送信装置には全ての前記複数の信頼度の全てに対応した複数の公開鍵が記憶されている情報伝送方法を実行するためのプログラムが記録された記録媒体であって、

前記情報送信装置において、前記情報受信装置に対して所定のデータを送るステップと、

前記情報送信装置において、前記所定のデータを送った返答として、前記情報

受信装置で前記秘密鍵により暗号化されたデータを受け取るステップと、

前記情報送信装置において、前記複数の公開鍵のいずれかを用いて、前記暗号化されたデータを解読するステップと、

前記情報送信装置において、前記解読されたデータと前記所定のデータとが一致しているかどうか判断するステップと、

前記判断するステップにおいて、前記解読されたデータと前記所定のデータとが一致した場合、前記解読手段で用いられた公開鍵に対応した信頼度が前記情報受信装置の信頼度であると判定するステップと、

前記判定された前記情報受信装置の信頼度に応じて制御しながら、前記情報送信装置から前記情報受信装置へ前記コンテンツを送るステップとを、

有する情報伝送方法を実行するためのプログラムが記録された記録媒体。

【請求項２１】

情報の守秘能力に応じてあらかじめ複数の信頼度に分類されており、前記複数の信頼度の各々に対応して著作権を有する証明コンテンツを有している対象装置の信頼度を判定する信頼度判定装置であって、

前記対象装置から所定のデータを受け取る受信手段と、

前記所定のデータから証明コンテンツを抽出する抽出手段と、

前記対象装置の信頼度の各々と前記対象装置が有する前記証明コンテンツとの対応関係が記憶されている記憶手段と、

前記記憶手段に記憶されている前記対応関係を参照して、前記受信手段により受け取った証明コンテンツが複数の信頼度のうちのいずれの信頼度に対応しているかを判断する判断手段と、

前記判断手段において判断された前記信頼度が前記対象装置の信頼度であると判定する判定手段とを、

有する信頼度判定装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報送信側から情報受信側へのコンテンツの伝送において、受信側

の著作権保護や守秘能力の保護に応じて、コンテンツの送信の可否を判断して、コンテンツの伝送を制御する方法に関する。

【０００２】

【従来の技術】

近年、映像音声機器のデジタル化が急速に進展し、映像音声などの情報信号をデジタル信号の形で機器間を伝送することも行われるようになってきた。そのような際に用いるデジタルインターフェイスとして、例えばＩＥＥＥ１３９４といった規格が定められている。しかし、デジタル信号の形での送受信が行われると、映画や音楽などのコンテンツが画質や音質の劣化なく伝送され、受信側の記録手段で記録した後の扱いは受信側に委ねられるため、著作権者の意図に反してそれらのコンテンツがコピーされて流通する可能性があるという問題があった。そこで、例えば特開平１０−３０４３３３号公報によれば、デジタルインターフェイスを持つ機器の中で著作権管理が確立している機器にのみ所定の鍵情報を保有させ、コンテンツデータの送信に先立って認証を求める側の機器（情報送信装置）はチャレンジデータを送り、それに対する、認証を受ける側の機器（情報受信装置）からの返答を解析することにより、この鍵情報を持っている機器にのみデータを送信することが提案されている.

【０００３】

【発明が解決しようとする課題】

しかし、受信機器において著作権保護について複数の信頼度レベルを設けることは考えられておらず、著作権者の意図に沿ってきめ細かい制御ができないという問題点があった。また、受信側の機器が鍵情報を盗用して用いて、あたかも著作権が保有された機器であるかのような返答が返した場合に対する対抗措置が不十分であった。

【０００４】

本発明は、機器に応じてコンテンツの送信の可否を決定し、コンテンツが簡単に外部に洩れそうなコンテンツ保護に対する安全性の弱い機器や、不特定な機器などにコンテンツを送信しないようにすることを目的とする。また、送ったコンテンツが不正に使用されることを防ぐことを目的とする。

【０００５】

【課題を解決するための手段】

本発明は、コンテンツを受信する情報受信側であるコンテンツ取扱装置を複数の異なる著作権保護レベル及び／又は守秘能力に従って分類し、信頼できる機器にのみ、情報送信側がコンテンツの送信を行えるようにするものである。また本発明は、送信側が、コンテンツを受信する情報受信側であるコンテンツ取扱装置を、著作権を有する認証コンテンツデータを用いて認証し、その認証結果に応じてコンテンツの送信の可否を決定し、コンテンツの送信を制御するものである。

【０００６】

【発明の実施の形態】

以下の実施の形態では、送信装置（認証機器）が単一の受信装置（コンテンツ取扱装置）に伝送路を介して接続されている場合について説明しているが、本発明は送信装置がインターネットその他の伝送媒体を介して複数のコンテンツ取扱装置（ＤＶＨＳやパソコンその他のコンテンツを記録したり再生したり加工したりすることの可能なあらゆる機器）に接続される場合を想定している。すなわち、本発明は、かかる様々な著作権保護レベルの機器に対してコンテンツを選択的に供給するものである。

<第１の実施の形態>

以下、図面を参照して、本発明の第１の実施の形態について説明する。図１は、本発明のコンテンツ伝送システムに係る第１の実施の形態における機器の構成図である。コンテンツ伝送システムは、情報送信装置と情報受信装置とを有し、情報送信装置と情報受信装置とは伝送媒体により接続されている。なお、本明細書において、送り先の信頼度を確認してコンテンツを送信する情報送信側を、情報送信装置、認証機器、信頼度判定装置などと呼ぶこともあり、一方、コンテンツを受信する情報受信側を、情報受信装置、証明機器、信頼度被判定装置、コンテンツ取扱装置などと呼ぶこともある。また、コンテンツをコンテンツ情報と呼ぶ場合もある。後述のように、情報受信装置の信頼度を判定するプロセス及び情報送信装置から情報受信装置にコンテンツ情報を送るときに、情報送信装置と情報受信装置の間を接続する伝送媒体上を情報が移動する。機器間の伝送媒体とし

ては、例えばＩＥＥＥ１３９４といったデジタルインターフェイスの規格が定められており、これを用いてもよい。また、ローカルエリアネットワークやインターネットなどによる接続や、さらには有線のみならず無線による接続でもよい。

【０００７】

第１の実施の形態の情報送信手段は、第１の記憶手段と、第１の送信手段と、受信手段と、第２の記憶手段と、解読手段と、判断手段と、判定手段と、制御手段と、第２の送信手段とを有する。第１の記憶手段３は、チャレンジデータとして情報受信装置２に送るための所定のデータが記憶されている手段である。第１の送信手段４は、第１の記憶手段３からチャレンジデータを読み出して、情報受信装置に送る手段である。受信手段５は、チャレンジデータの返答として情報受信装置から送られてくるレスポンスデータ受け取る手段である。第２の記憶手段６は、情報受信装置側の複数の信頼度の全てに対応した複数の公開鍵が記憶されている手段である。情報受信装置２は著作権保護レベル及び／又は情報の守秘能力に応じて、信頼度が規定されている。解読手段７は、複数の公開鍵を用いて、情報受信装置２から送られてくるレスポンスデータを解読する手段である。判断手段８は、チャレンジデータと解読手段７により解読されたデータとが一致しているか否かを判断する手段である。判定手段９は、判断手段８がチャレンジデータと解読手段７により解読されたデータとが一致していると判断した場合、解読手段７で用いられた公開鍵に対応した信頼度が前記情報受信装置２の信頼度であると判定する手段である。制御手段１０は、判定手段９により判定された情報受信装置２の信頼度に応じて、情報受信手段２へのコンテンツ情報の送信を制御する手段である。第２の送信手段１１は、制御手段１０の制御の下で、コンテンツ情報を情報受信装置２に送信する手段である。また、上記の情報送信装置からコンテンツデータを送信する手段（制御手段１０、送信手段１１）を取り除いて、情報受信側の信頼度を判定することを特徴とする信頼度判定装置とすることも可能である。

【０００８】

一方、情報受信手段は、第１の受信手段と、記憶手段と、暗号化手段と、送信手段と、第２の受信手段とを有する。第１の受信手段１２は、情報送信装置１か

ら送られるチャレンジデータ（所定のデータ）を受け取る手段である。記憶手段１３は、複数の信頼度の特定の１つに対応した秘密鍵が記憶されている手段である。秘密鍵は、あらかじめ情報受信装置２の著作権保護レベル及び／又は守秘能力に対応した信頼度に応じて、記憶手段１３に与えられているか又は設定されている。また、記憶手段以外に秘密鍵の情報を記憶させる以外に、ハードウェアから抽出される特有の情報、例えばシリアルナンバーなどを秘密鍵とすることも可能である。暗号化手段１４は、秘密鍵を用いてチャレンジデータを暗号化してレスポンスデータを作成する手段である。送信手段１５は、暗号化手段１４で暗号化されたレスポンスデータを情報送信装置１に送る手段である。第２の受信手段１６は、暗号化されたデータを送信手段１５により送った結果、情報送信装置１から送られてくるコンテンツ情報を受け取る手段である。また、上記の情報受信装置１からコンテンツデータを受信する手段（第２の受信手段１６）を取り除いて、情報送信側に信頼度を判定されることを特徴とする信頼度被判定装置とすることも可能である。

【０００９】

本発明においては、機器の信頼度に応じて信頼度を分類する鍵を、認証機器（情報送信側）とコンテンツ取扱装置（情報受信側）の双方に与え、情報受信側の鍵の信頼度に基づいて、情報受信側を分類する。機器の分類方法における指標となる機器の信頼度とは、著作権保護が十分確保できるかに関する信頼度であり、該当する機器が取り扱う重要な情報が、機器の外部から、あるいは内部で容易に盗み見ることができるか否かを基準とする。また、信頼度は、著作権の有無に係わらず、その機器が扱う情報の守秘能力、すなわち機器の外部に対して情報を漏洩しない能力であるとも言える。

【００１０】

具体的には、例えば機器を分類するための信頼度の指標としてのレベルを、機器の構成上から、次のような条件により分ける。

レベル１：外部インターフェイスを介して暗号化されていないコンテンツデータを送り出すことができる。

レベル２：外部インターフェイスを介して暗号化されていないコンテンツデー

タを送り出すことはないものの、暗号化されていないコンテンツデータが、内部の基盤上のコネクタなどや、機器内部のバスに直接出力され、ある程度の知識を有する者がそれらの場所からデータを容易に抜き取ることができる。

レベル３：暗号化されていないコンテンツデータが基盤上において、容易に取り出せる所には出力されてはいないが、存在はしている（例えばＢＧＡパッケージなどの形のＬＳＩ間を基盤の内層を通る配線で接続しているものなど）。

レベル４：暗号化されていないコンテンツデータはＬＳＩ内部にのみ存在し、その外へ出すコンテンツデータは常に暗号化されている。

ここでは、レベルの値が大きくなるほど、著作権保護に関する信頼度の度合いが高くなっている。

【００１１】

また、機器の分類法としては、機器のカテゴリー（パーソナルコンピュータ、テレビジョン受像機、ＤＶ方式ビデオカセットレコーダ、Ｄ−ＶＨＳ方式ビデオカセットレコーダなど）を用いてもよい。ここで、ある方式の機器は必ず上記のレベル４の構成とするといったことをその方式の規格で規定し、その方式の機器は必ずそのレベルのいずれかに含まれることを、規格のライセンサーがライセンシーに対して要求することで、その機器のレベルが保証される。このようにレベルが保証されない機器については、個別に相当するカテゴリーに分類する（例えば、テレビジョン受像機であっても、その機能においてパーソナルコンピュータの場合と同様にコンテンツの加工・複製ができるものがあったとすると、この機器はパーソナルコンピュータとして分類する）。各機器に対する分類に従った固有情報の付与は、特定の機関あるいは会社が一括して行い、この付与が行われていない機器は信頼度の判定において最も信頼度の低いレベルとみなすことにより、世の中に存在する全ての機器の信頼度の判定を行うことができる。

【００１２】

以下に、機器間の伝送において、このような信頼度の認証を行う際の第１の実施の形態を説明する。第１の実施の形態は、信頼度に応じて複数の秘密鍵及び公開鍵を設定し、信頼度に応じて異なる鍵を情報受信装置に与えておくものである。ここで暗号化は公開鍵暗号の手法をとるものとする。この手法においては、他

に知られても良い公開鍵と、その機器の外には漏れないようにしてある秘密鍵の組が用いられ、組となる公開鍵、秘密鍵のどちらか一方で暗号化された情報は、他方で解読できるようになっている。ここで、公開鍵ｎ（ｎは自然数）と秘密鍵ｎが組になっており、信頼度ｎの機器はあらかじめ秘密鍵ｎが与えられている。以下に説明する第１の実施の形態では、情報受信側の機器の信頼度はＮ段階で規定されており、今対象とする情報受信側の信頼度がｋ（ｋは１からＮまでの自然数）で設定されている場合を説明する。また、信頼度の最も低い機器をｋ＝１、信頼度が最も高い機器をｋ＝Ｎとし、信頼度が上がるにつれてｋの値も大きくなる。

【００１３】

図２は、図１で示した本発明のシステムに係る第１の実施の形態における情報送信側の動作を説明するフローチャートである。ステップＳ１０１において、チャレンジデータを情報受信側に送る。チャレンジデータは、情報送信側の記憶手段に記憶されている。さらにセキュリティを高めるために、このチャレンジデータをさらに暗号化してから、情報受信側に送出してもよい。ステップＳ１０２において、ｋ＝１及びＬ＝１と設定する。ｋは、後に行うステップＳ１０４でのレスポンスデータの解読に用いられる公開鍵に対応する信頼度のパラメータであり、Ｌは、情報送信側が判断する情報受信側の信頼度である。ステップＳ１０３において、情報送信側は、情報受信側から送られたレスポンスデータを受け取る。後で説明するが、レスポンスデータは、情報受信側が情報送信側に送るものである。

【００１４】

ステップＳ１０４において、情報送信側は、情報送信側が有する公開鍵ｋを用いてレスポンスデータを解読する。公開鍵ｋは信頼度ｋの鍵であり、信頼度ｋの公開鍵ｋは信頼度ｋの秘密鍵と同一、あるいは同等の機能を果たすものである。ステップＳ１０５において、ステップＳ１０４で公開鍵ｋ（ｋ∈Ｌ）により解読されたデータ（解読データ）と、ステップＳ１０１で情報受信側に送信したチャレンジデータとが一致しているか否か判断する。ステップＳ６において、ステップＳ４で解読されたデータと所定のデータとが一致した場合、ステップＳ５でレ

スポンスデータを解読した公開鍵ｋの信頼度ｋが情報受信側の信頼度に等しいと判定し、Ｌ＝ｋとする。ステップＳ１０７において、ステップＳ１０４で復号されたデータと所定のデータとが一致しない場合、ステップＳ１０５でレスポンスデータを解読した公開鍵ｋの信頼度ｋが情報受信側の信頼度とは異なると判定し、ｋ＝ｋ＋１とする。すなわち、例えば、ｋ＝１だったならばｋ＝２とする。これにより、例えば公開鍵１で解読されたデータがチャレンジデータと一致しなければ、公開鍵２でレスポンスデータを解読し、解読されたデータとチャレンジデータとが一致するか否かを再び判断することになる。

【００１５】

ステップＳ１０８において、ｋ＞Ｎであるか否かを判断する。ｋ≦Ｌの場合、ステップＳ１０４に戻り、信頼度の異なる公開鍵でステップＳ１０４以降のステップを行う。一方、ｋ＞Ｌの場合、すなわち、情報送信側が有するｋ＝１～Ｌの全ての公開鍵でレスポンスデータを解読した場合、認証機器は証明機器のレベルを最も信頼度の低いレベル１とみなす。こうしてステップＳ１０４～Ｓ１０８において、認証機器が有する全ての公開鍵ｋ（ｋ∈Ｌ）でレスポンスデータを解読し、解読されたデータとチャレンジデータとが一致するか否かを判断することが可能となる。また、ステップＳ１０９において、チャレンジデータ送信後の待ち時間があらかじめ設定された待ち時間であるｔｗ時間を超えた場合、すなわちチャレンジデータの送信後、あらかじめ設定した所定時間を経過してもレスポンスデータが戻って来ない場合、ステップＳ１０４～Ｓ１０８を行わず、ステップＳ１０に飛ぶ。したがって、レスポンスデータが戻って来ない場合、情報送信側は、情報受信側の信頼度を初期値であるＬ＝１、すなわち最も低い信頼度とみなすことになる。以上が、情報送信側が情報受信側の信頼度を判定する過程であり、このステップまでを行う情報送信側の装置を信頼度判定装置としてまとめることが可能である。

【００１６】

本実施の形態では、ステップＳ１０２でｋ＝１と設定し、続いてｋ＝２、３…と昇順させて比較していくが、結果的にステップＳ１０４において、情報送信側が有する全ての公開鍵（ｋ＝１～Ｌ）でレスポンスデータが解読可能であるなら

ば、公開鍵によるチャレンジデータの解読はどのような順序で行っても構わない。また、ステップＳ１０２でＬの値を設定せずに、ステップＳ１０８でｋ＞Ｌの場合及びステップＳ１０９を行う場合にＬ＝１とすることも可能である。

【００１７】

上記の信頼度判定の過程により、情報送信側は、送信受信側の信頼度を判定してコンテンツ情報の送信を行う。今、例えばL_p以上の信頼度を有する機器にのみに対して、情報送信側はコンテンツ情報を送信するよう設定されているとする。ステップＳ１１０において、ステップＳ１０１～Ｓ１０９での信頼度の判定で得られた情報受信側の信頼度Ｌが、コンテンツ情報が送信可能な信頼度以上か否か、すなわち$L \geqq L_p$か否かを判定する。$L \geqq L_p$の場合、ステップＳ１１１において情報受信側に対してコンテンツ情報の送信を開始する。この場合、例えば送りたいコンテンツ情報のヘッダなどに記録されている信頼度情報L_pと情報受信側の信頼度Ｌを比較して、$L \geqq L_p$ならばコンテンツ情報の送信処理を行わないようにする。

【００１８】

また、例えばペイ・パー・ビューにより提供される番組のコンテンツ情報をレベル４、ペイ・パー・ビューではない映画、ドラマなどのコンテンツ情報をレベル３、ペイ・パー・ビューではないニュースなどのコンテンツ情報をレベル２として、同一の信頼度を有するコンテンツ情報をそれぞれ同一の記憶手段に蓄積しておき、情報受信側の信頼度Ｌに対応して記録手段へのアクセスを制限することも可能である。さらに、ビデオソフト再生の場合は、例えば検出穴を設ける、バーコードが印刷されたシールを貼る、ＩＣメモリをカセットに装着するなどして、送信可能な信頼度情報をカセットなどの記録媒体上に載せておき、コンテンツ情報を送る際にその信頼度情報を読み取ることも可能である。ステップＳ１１２において、送信すべきコンテンツ情報が全て送信されたら、情報受信側の信頼度の判定及び情報受信側へのコンテンツ情報の送信は終了となる。一方、$L < L_p$の場合、ステップＳ１１３において、情報受信側に対して送信できない旨の警告を送信する。この場合、警告のメッセージを送信してもよいし、また、あらかじめ送信不可能の場合に送る信号を定めておいて、その信号を情報受信側に送信し

てもよい。これにより情報受信側が所定レベル以上の信頼度を満たした場合、すなわち、コンテンツ情報が不正に複製されたり改竄されたりすることのない機器であるという確信が情報送信側で得られた場合に、情報送信側から情報受信側にコンテンツ情報を送るようにすることが可能となる。

【００１９】

図３は、図１で示した本発明のシステムに係る第１の実施の形態における情報受信側の動作を説明するフローチャートである。ステップＳ２０１において、チャレンジデータを情報送信側から受け取る。ステップＳ２０２において、秘密鍵ｋを用いてステップＳ２０１で受信したチャレンジデータを暗号化して、暗号化データを作成する。ステップＳ２０３において、ステップＳ２０２で作成された暗号化データをレスポンスデータとして、情報送信側に送る。以上が、信頼度を判定する過程における情報受信側の動作であり、このステップまでを行う情報受信側の装置を信頼度被判定装置としてまとめることが可能である。秘密鍵ｋを用いてレスポンスデータを作成し、情報送信側に送ることにより、情報送信側に情報受信側の機器の信頼度を伝えることが可能となる。

【００２０】

上記の信頼度判定の過程により、情報受信側の信頼度に応じて、情報送信側からコンテンツ情報の送信が行われるか否かが決定される。情報送信側からコンテンツ情報の送信が始まった場合、ステップＳ２０４において、情報受信側はコンテンツ情報の受信を開始する。ステップＳ２０５において、受信してコンテンツ情報に対して、記録媒体への記録やディスプレイへの表示など所定のプロセスを行う。ステップＳ２０６において、コンテンツ情報の受信が終了した場合、ステップＳ２０７において、ステップＳ２０５で行っていた所定のプロセスを終了する。

【００２１】

＜第２の実施例＞

次に第２の実施例を図３に基づいて説明する。この例では、情報送信側の信頼度に応じて、信頼度のレベルごとに異なる固有のデータをあらかじめ各情報送信側に与えておく。この固有データは、詩などの文章、音楽、画像、ロゴなど、そ

れ自身で著作権を主張できる内容を含んだコンテンツ情報で構成されていてもよい。なお、本明細書では、このレベルによって異なる固有データを証明用コンテンツ情報と呼ぶこともある。情報送信側が情報受信側の信頼度を判定するプロセスにおいて、情報受信側は、情報送信側からの問いかけに対して著作権を有する証明コンテンツ情報を含んだデータを情報送信側に返す。もし、ある情報受信側が証明コンテンツ情報を与えられたものではなく、しかし、この証明コンテンツ情報を不正に盗用して情報送信側に対して送信を行った場合、証明用として用いられた証明コンテンツ情報に係る著作権を侵害して、情報受信側から情報が送信されたことになり、証明コンテンツ情報を不正に用いたということをさらに主張しやすくなるという効果がある。

【0022】

第2の実施の形態における情報送信側及び情報受信側の構成について説明する。基本的には第1の実施の形態と同じであるが、第2の実施の形態は、特に、情報受信側からのレスポンスデータから証明コンテンツ情報を抽出する抽出手段が存在していることが特徴である。また、チャレンジデータを送る第1の送出手段がなく、したがって情報送信側からのチャレンジデータの送信がなくても、まず情報受信側が固有データを情報送信側に送信して認証を働きかけてもよい。

【0023】

まず、第2の実施の形態における情報受信側の動作について説明する。図5は、本発明のシステムに係る第2の実施の形態における情報受信側の動作を説明するフローチャートである。ステップS401において、チャレンジデータを情報送信側から受け取る。ステップS402において、情報受信側が有する所定の固有データと、ステップS401で受信したチャレンジデータとの間で所定の演算を行う。この演算は例えば乗算などが挙げられるが、情報送信側に送った場合、情報送信側での演算により情報受信側の固有データがどの信頼度を示すものであるかが識別可能であれば、どのような演算でも可能である。ステップS403において、ステップS2で作成された暗号化データをレスポンスデータとして、情報送信側に送る。以上が、信頼度を判定する過程における情報受信側の動作である。情報受信側は固有データkを用いてレスポンスデータを作成し、情報送信側

に送ることにより、情報送信側に情報受信側の機器の信頼度を伝えることが可能となる。その後ステップＳ４０４以降のコンテンツ情報の受信に関しては第１の実施の形態と同様のステップを行う。

【００２４】

次に、第２の実施の形態における情報送信側の動作について説明する。図４は、本発明のシステムに係る第２の実施の形態における情報送信側の動作を説明するフローチャートである。

ステップＳ３０１～Ｓ３０３の動作は、第１の実施の形態のステップＳ１０１～Ｓ１０３の動作と同一である。ステップＳ３０４において、所定の演算を行うことによりレスポンスデータから固有データを抽出する。この演算は、例えば情報受信側でレスポンスデータを作成する際に用いられた演算の逆演算などである。ステップＳ３０４で固有データを抽出する代わりに、各レベルの固有データとチャレンジデータとに対して情報受信側で行う演算と同一の演算を行って、レスポンスデータに対応するデータを情報送信側で作成し、さらに、ステップＳ３０４で作成したデータと受信したレスポンスデータとが一致するか否か判断してもよい。

【００２５】

ステップＳ３０５において、情報送信側に記憶されている信頼度ｋを示す固有データとステップＳ４で抽出された固有データが一致しているか否か判断する。ステップＳ３０６において、情報送信側に記憶されている信頼度ｋを示す固有データとステップＳ３０４で抽出された固有データが一致した場合、情報送信側に記憶されているステップＳ３０５で用いられた固有データの信頼度ｋが情報受信側の信頼度に等しいと判定し、Ｌ＝ｋとする。情報送信側で抽出された固有データがコンテンツ内容のデータである場合、このコンテンツ内容のデータ（証明用コンテンツ情報）が著作権を持ったコンテンツであることを明確にするためには、証明用コンテンツ情報を何らかの形で使用者に提示する機会を設けるとよい。例えば、認証が終わってから一定の期間において、証明コンテンツ情報のコンテンツ内容が外部に表出されるようにする。すなわち、ステップＳ３０７において、抽出された固有データをコンテンツ表出部に送る。証明コンテンツ情報のコン

テンツ内容がロゴなどの画像である場合には、その画像が情報送信側に接続された、あるいは情報送信側に内蔵されたディスプレイに例えば数秒間といった短い時間表示されるようにし、詩のような文章の場合には、その文章の文字がディスプレイに表示されたり、音声に変換されてスピーカから発せられたりし、音楽信号の場合には、そのメロディがスピーカから発せられるようにすればよい。また、情報受信側の表出部に証明コンテンツ情報が表示されるようにすることも可能である。

【００２６】

一方、ステップＳ３０８において、情報送信側に記憶されている信頼度ｋを示す固有データとステップＳ３０４で抽出された固有データが一致しない場合、情報送信側に記憶されているステップＳ３０５で用いられた固有データの信頼度ｋが情報受信側の信頼度とは異なると判定し、ｋ＝ｋ＋１とする。すなわち、例えば信頼度１の固有データがステップＳ３０４で抽出された固有データと一致しなければ、信頼度２の固有データとステップＳ３０４で抽出された固有データとが一致するか否かを再び判断することになる。

【００２７】

ステップＳ３０９において、ｋ＞Ｎであるか否かを判断する。ｋ≦Ｌの場合、ステップＳ３０５に戻り、信頼度の異なる固有データでステップＳ３０５以降のステップを行う。一方、ｋ＞Ｌの場合、すなわち、情報送信側が有するｋ＝１～Ｌの全ての信頼度の固有データと、ステップＳ３０４で抽出した固有データとが一致しているか否かの判断がなされた場合、情報送信側は、情報受信側の信頼度を最も低い信頼度Ｌ＝１とみなす。こうしてステップＳ３０４～Ｓ３０９において、情報送信側が有する全ての固有データｋ（ｋ∈Ｌ）とレスポンスデータから抽出された固有データとが一致するか否かを判断することが可能となる。第２の実施の形態におけるステップＳ３１０は、第１の実施の形態におけるステップＳ１０９と同一であり、以上が第２の実施の形態の信頼度判定の過程である。

【００２８】

上記のようにして、情報送信側は、送信受信側の信頼度を判定してコンテンツ情報の送信を行う。第２の実施の形態におけるコンテンツ情報の送信の過程であ

るステップＳ３１１～Ｓ３１４は、第１の実施の形態と同一である。また第２の実施の形態においても、ステップＳ３０２でｋ＝１と設定し、続いてｋ＝２、３…と昇順させて比較していくが、結果的にステップＳ３０５において、情報送信側が有する全ての固有データ（ｋ＝１～Ｌ）とステップＳ３０４で抽出された固有データとが一致するか否かの判断が可能ならば、情報送信側が有する固有データと抽出された固有データとの比較はどのような順序で行っても構わない。また、ステップＳ３０２でＬの値を設定せずに、ステップＳ３０９でｋ＞Ｌの場合及びステップＳ３１０を行う場合にＬ＝１とすることも可能である。

【００２９】

また、情報受信側を複数の信頼度に分類し、著作権の存在する固有データを各信頼度に対応させているが、複数の信頼度に分類する必要はなく、認証に際して著作権の存在する固有データを用いるだけでもよい。これによって、不正に情報受信側から情報送信側に認証しようとする者は、認証の際に、著作権の存在する固有データを伝送することになり、著作権を不法に侵害することになる。その結果、不正行為を訴える場合に、有利に働くという作用効果がある。

【００３０】

＜第３の実施例＞

次に、第３の実施例について説明する。これは第２実施例に加えて、情報受信側からレスポンスデータを送る際に、ハッシュ関数などの暗号化に関する関数を使うデジタル署名の手法を用いてデータを作成し、レスポンスデータ伝送中の改竄を検出できるようにし、また、ハッシュ関数による圧縮結果を用いて情報受信側の信頼度を判定するものである。ここで、ハッシュ関数とはデジタル情報をこの関数で変換することにより決まった長さのデータに圧縮する関数で、逆関数が存在しないので、いったんハッシュ関数により圧縮して得られたダイジェスト版についてはそれを再び元のデジタル情報に戻すことはできないという性質を有するものである。ハッシュ関数の例としては、１６０ｂｉｔのハッシュ値を生成するものとして米国ＮＳＡ（ｔｈｅ　Ｎａｔｉｏｎａｌ　Ｓｅｃｕｒｉｔｙ　Ａｇｅｎｃｙ）で考案されたＳＨＡ－１（Ｓｅｃｕｒｅ　Ｈａｓｈ　Ａｌｇｏｒｉｔｈｍ　１）などがある。

【００３１】

第３の実施の形態における情報送信側及び情報受信側は、第１又は第２の実施の形態とほぼ同一の構成である。しかし、特に第３の実施の形態における情報送信側及び情報受信側は、双方とも、例えばハッシュ関数のような暗号化に用いられる演算手段を有していることが特徴である。第２の実施の形態に示した固有データを、さらにハッシュ関数により圧縮し、より信頼度の認証のセキュリティを高めている。

【００３２】

情報受信側は受信したチャレンジデータと情報受信側が有する信頼度ｋを示す固有データとの間で所定の演算を行い（第１の暗号化）、レスポンスデータの主要部を作成する。さらに情報受信側は、情報受信側が有する信頼度ｋを示す固有データをハッシュ関数により圧縮し、署名データを作成する。この署名データを暗号化し（第２の暗号化）、前記レスポンスデータの主要部に付加部として付加する。情報受信側は、こうして作成したデータをレスポンスデータとして情報送信側に送る。

【００３３】

一方、情報送信側は、まず、第２の暗号化が施された付加部の暗号化を解読（第２の暗号化の解読）する。さらに、第１の暗号化が施されたレスポンスデータの主要部をチャレンジデータとの演算により解読（第１の暗号化の解読）して固有データを抽出する。こうして抽出された固有データが情報受信側で用いたのと同じハッシュ関数で圧縮され、先の第２の暗号化の解読による解読結果と比較される。レスポンスデータ送信中に改竄がなければ、これらは一致するはずである。もし一致しなければ、情報送信側の信頼度は最も低いレベルとみなされ、一致した場合には、その結果が、情報送信側にあらかじめ蓄積されている各レベルの固有データについてのハッシュ関数による圧縮関数の情報と比較され、情報受信側の信頼度が判定される。また、第２の実施の形態と同様に、情報送信側で解読された情報受信側の固有データがコンテンツ内容のデータである場合には、そのコンテンツ内容が外部に表出される。

【００３４】

その他の方法として、証明用コンテンツの利用方法として、証明用コンテンツ情報の少なくとも一部を鍵の一部として用いたり、また、例えば第１の実施の形態のような方法で情報送信側から送られるチャレンジデータとそれに対する情報受信側からのレスポンスデータの比較判断が行われた後、さらに所定のコンテンツが暗号化されて情報受信側から情報送信側へと送られ、その内容を情報送信側で確認して初めて信頼度の判定が完了したりするようにしてもよい。

【００３５】

さらに、チャレンジデータとして、これから送ろうとしている情報に対して情報送信側がどのレベル以上の信頼度であることが必要かを示すデータを送り、情報受信側はそのレベル以上の信頼度を持っているか否かを示すデータをレスポンスデータとして返すようにしてもよい。また、この方法の場合、必要なレベル以上の信頼度を持っていない場合には、情報受信側はレスポンスデータを返すこと自体を行わないようにしてもよい。機器間の接続においてこのようなプロセスにより機器の信頼度を判定し、さらに各機器が保有している、あるいは外部から送られてくる情報のヘッダなどの所定の個所に、どのレベルの機器までその送信を許すかに関する情報（許可情報）を含ませておくことにより、上記の方法で判定した送信対象機器のレベルと、送信しようとしている情報の許可情報を比較して、その確報の送信の可否を決定することができ、その情報の重要性に応じて、情報が盗まれる可能性のある機器への送信を防止することができる。

【００３６】

【発明の効果】

以上説明したように、本発明ではコンテンツを受信する情報受信側であるコンテンツ取扱装置を複数の異なる著作権保護レベル及び／又は守秘能力に従って分類し、信頼できる機器にのみ、情報送信側がコンテンツの送信を行えるようにしている。また本発明では、送信側が、コンテンツを受信する情報受信側であるコンテンツ取扱装置を、著作権を有する認証コンテンツデータを用いて認証し、その認証結果に応じてコンテンツの送信の可否を決定し、コンテンツの送信を制御している。その結果、機器に応じてコンテンツの送信の可否を決定し、コンテンツが簡単に外部に洩れそうなコンテンツ保護に対する安全性の弱い機器や、不特

定な機器などにコンテンツを送信しないようにすることができる。また、送ったコンテンツが不正に使用されることを防ぐことが可能となる。

【図面の詳細な説明】

【図１】

本発明のコンテンツ伝送システムに係る第１の実施の形態における機器の構成図である。

【図２】

図１で示した本発明のコンテンツ伝送システムに係る第１の実施の形態における情報送信側の動作を説明するフローチャートである。

【図３】

図１で示した本発明のシステムに係る第１の実施の形態における情報受信側の動作を説明するフローチャートである。

【図４】

本発明のシステムに係る第２の実施の形態における情報送信側の動作を説明するフローチャートである。

【図５】

本発明のシステムに係る第２の実施の形態における情報受信側の動作を説明するフローチャートである。

【符号の説明】

１　情報送信装置（認証機器）

２　情報受信装置（コンテンツ取扱装置）

３　第１の記憶手段

４　第１の送信手段

５　受信手段

６　第２の記憶手段

７　解読手段

８　判断手段

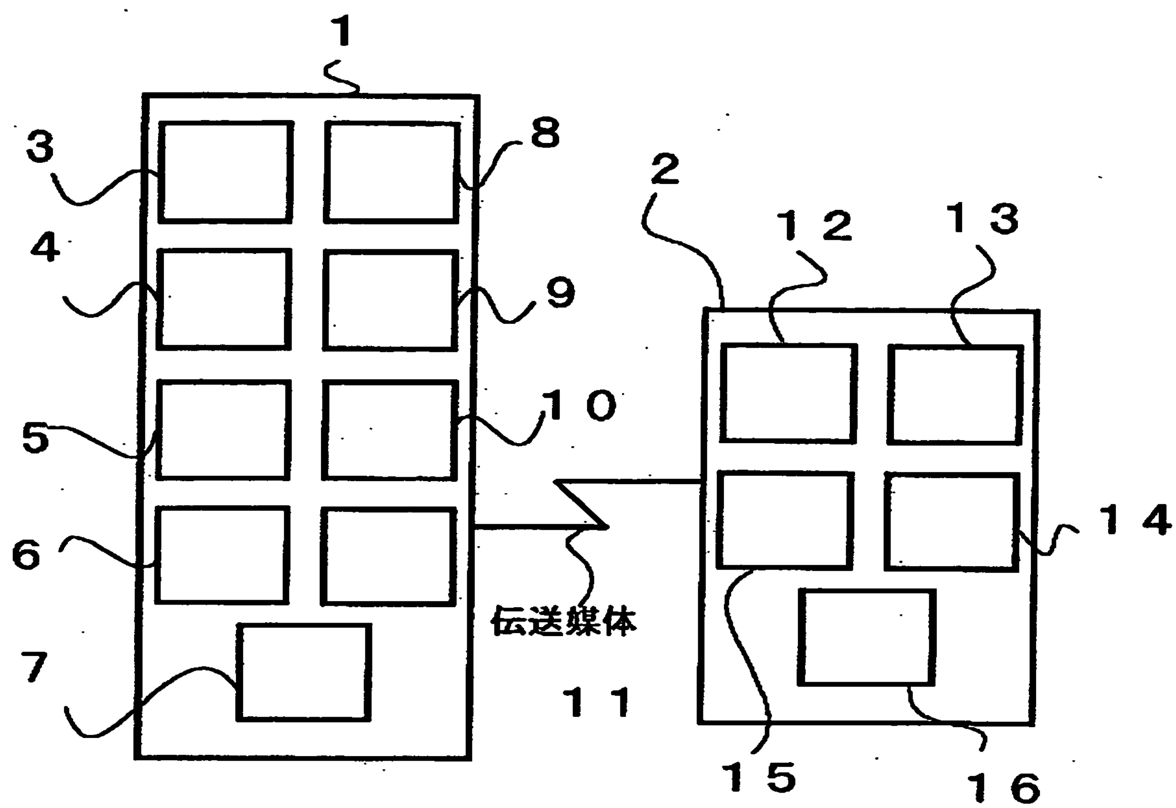
９　判定手段

１０　制御手段

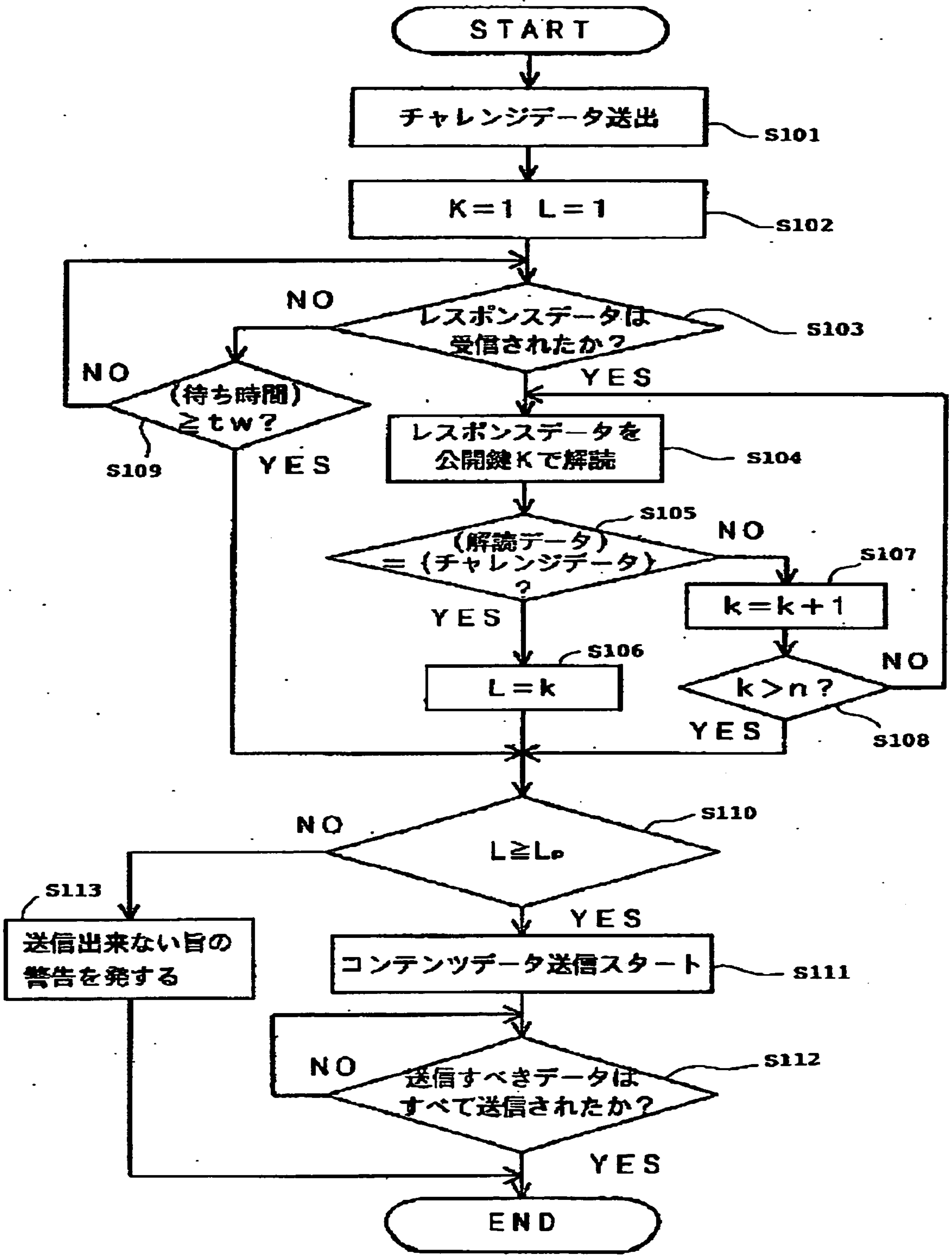
１１　第２の記憶手段
１２　第１の受信手段（情報受信側）
１３　記憶手段（情報受信側）
１４　暗号化手段
１５　送信手段（情報受信側）
１６　第２の受信手段（情報受信側）

【書類名】　　図面

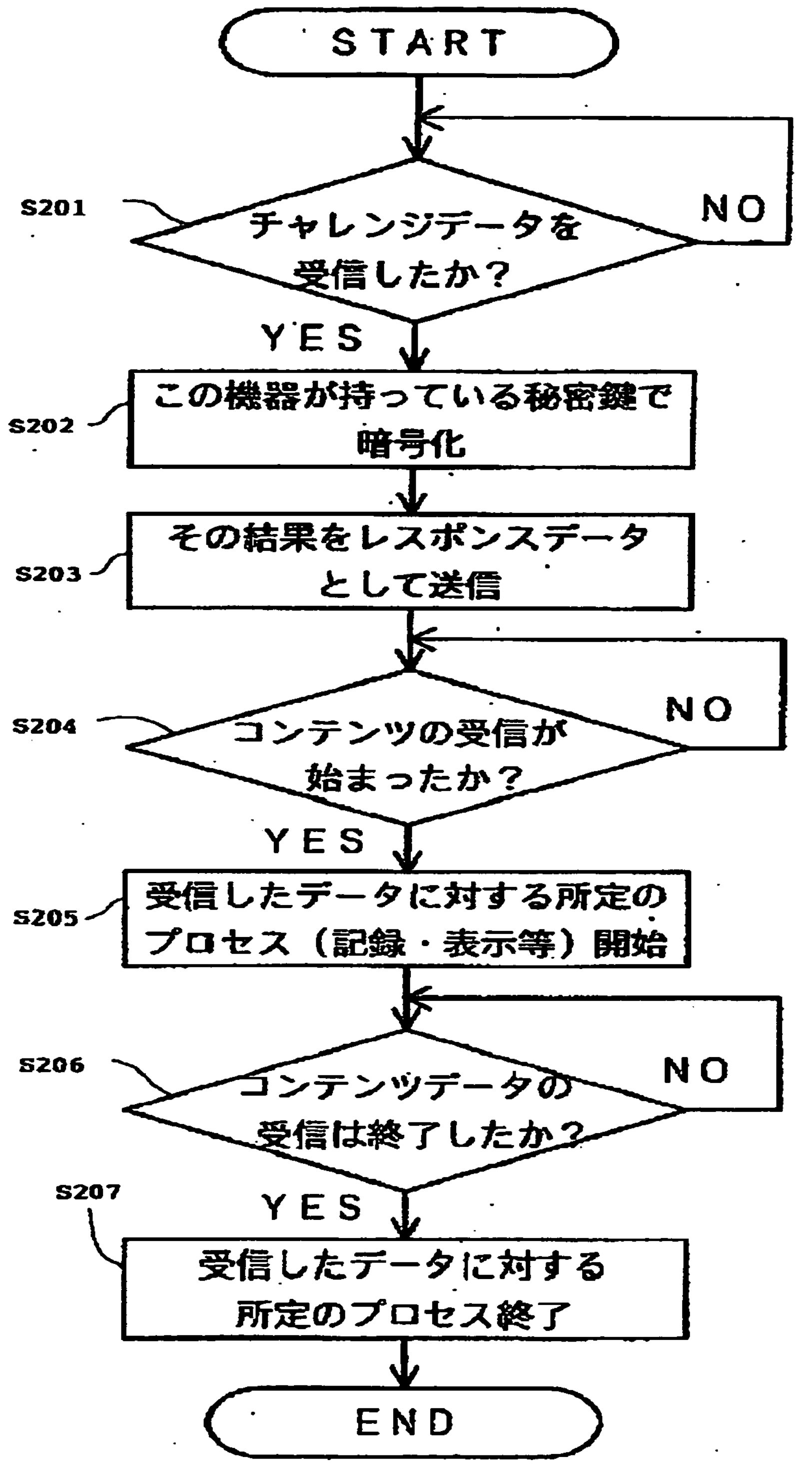
【図１】



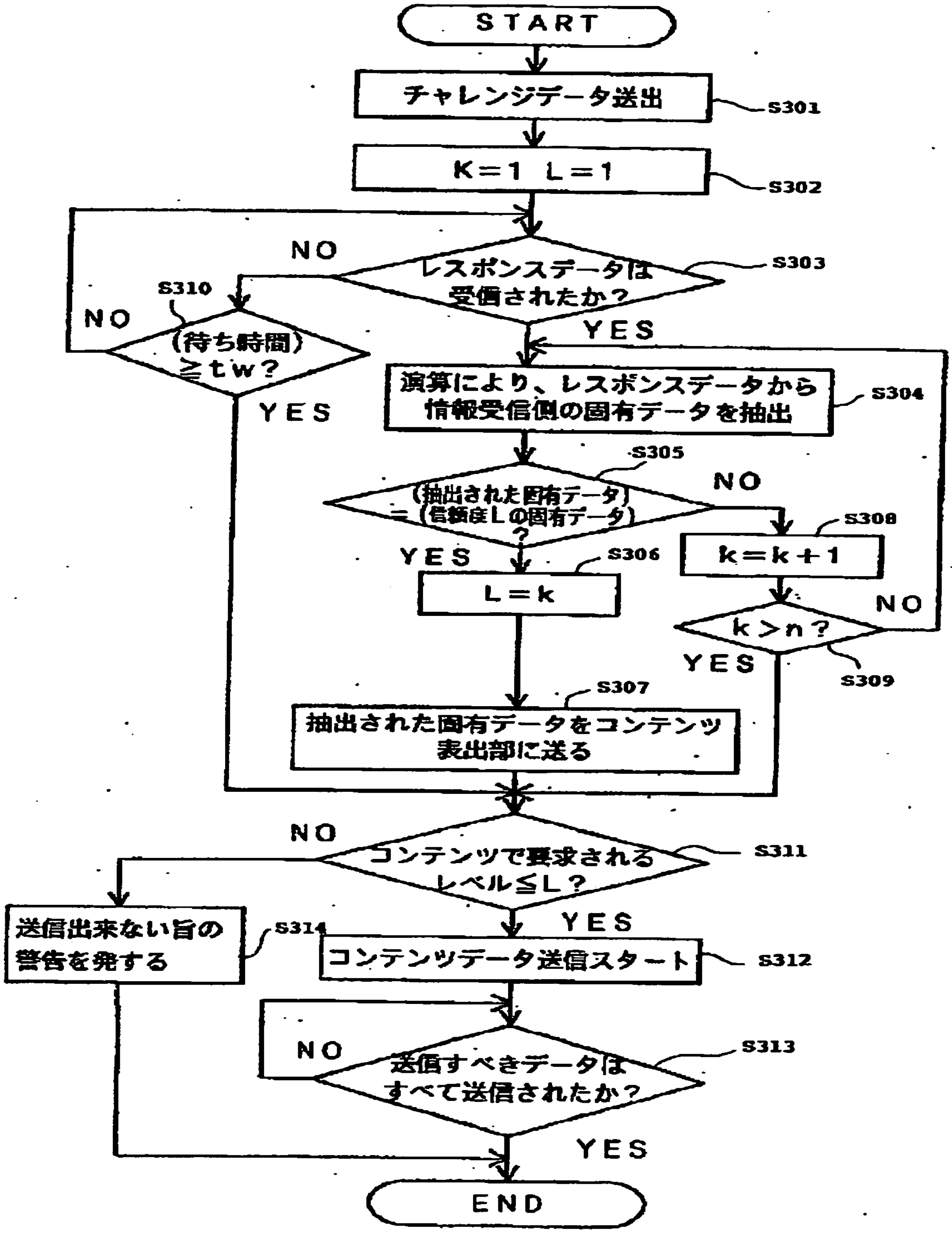
【図２】


START
チャレンジデータ送出
S101
K=1 L=1
S102
レスポンスデータは受信されたか？
S103
NO
YES
(待ち時間)≧tw？
S109
NO
YES
レスポンスデータを公開鍵Kで解読
S104
(解読データ)＝(チャレンジデータ)？
S105
NO
YES
k=k+1
S107
k>n？
S108
NO
YES
L=k
S106
L≧L0
S110
NO
YES
送信出来ない旨の警告を発する
S113
コンテンツデータ送信スタート
S111
送信すべきデータはすべて送信されたか？
S112
NO
YES
END

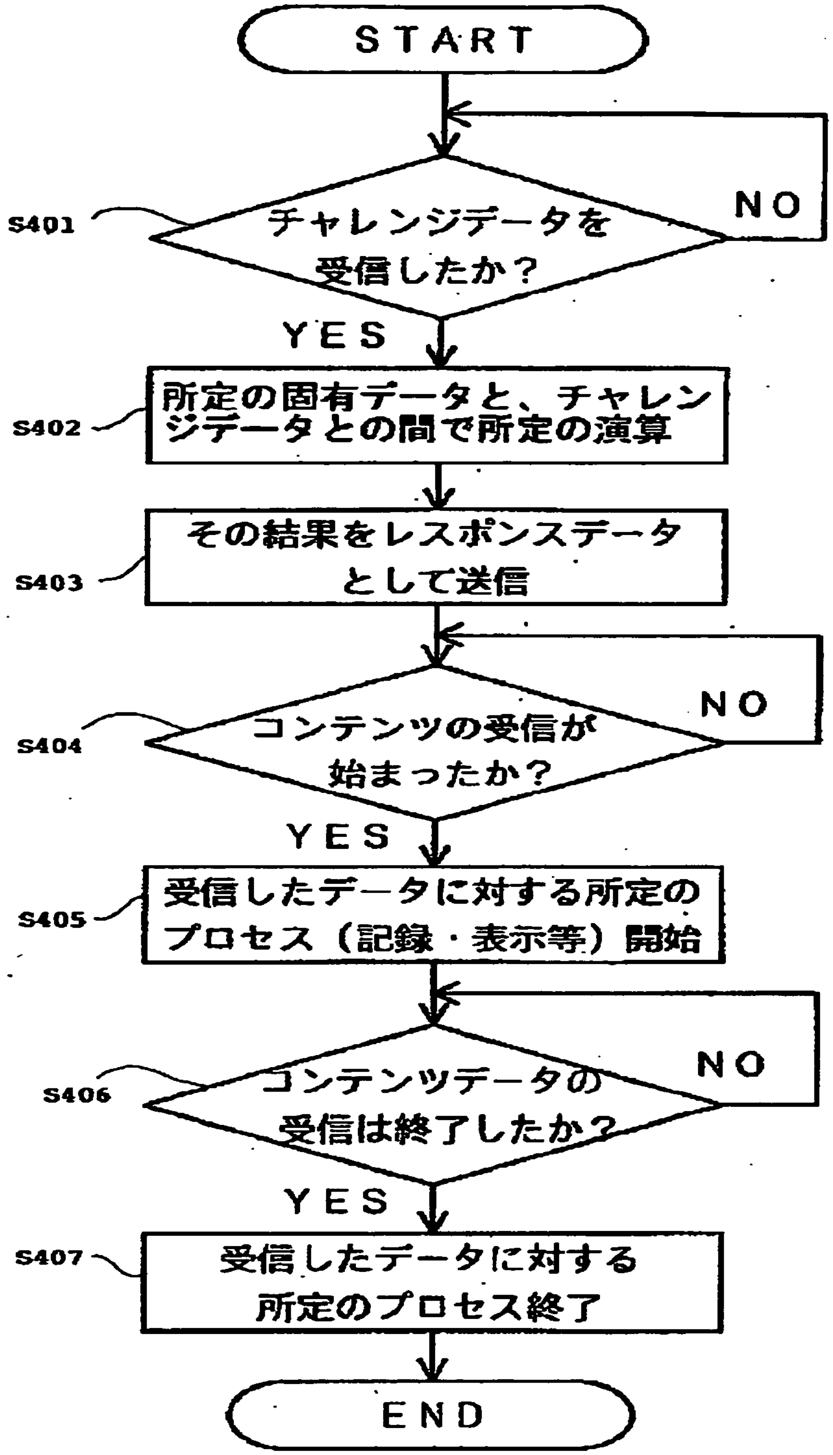
【図３】


START
S201
チャレンジデータを受信したか？
NO
YES
S202
この機器が持っている秘密鍵で暗号化
S203
その結果をレスポンスデータとして送信
S204
コンテンツの受信が始まったか？
NO
YES
S205
受信したデータに対する所定のプロセス（記録・表示等）開始
S206
コンテンツデータの受信は終了したか？
NO
YES
S207
受信したデータに対する所定のプロセス終了
END

【図４】


START
チャレンジデータ送出
S301
K＝1 L＝1
S302
レスポンスデータは受信されたか？
S303
NO
YES
S310
（待ち時間）≧tw？
NO
YES
演算により、レスポンスデータから情報受信側の固有データを抽出
S304
（抽出された固有データ）＝（信頼度Lの固有データ）？
S305
NO
YES
S308
k＝k＋1
S306
L＝k
k＞n？
NO
YES
S309
S307
抽出された固有データをコンテンツ表出部に送る
コンテンツで要求されるレベル≦L？
S311
NO
YES
送信出来ない旨の警告を発する
S314
コンテンツデータ送信スタート
S312
送信すべきデータはすべて送信されたか？
S313
NO
YES
END

【図５】


START
S401
チャレンジデータを受信したか？
NO
YES
S402
所定の固有データと、チャレンジデータとの間で所定の演算
S403
その結果をレスポンスデータとして送信
S404
コンテンツの受信が始まったか？
NO
YES
S405
受信したデータに対する所定のプロセス（記録・表示等）開始
S406
コンテンツデータの受信は終了したか？
NO
YES
S407
受信したデータに対する所定のプロセス終了
END

【書類名】　　　要約書
【要約】
【課題】　機器に応じてコンテンツの送信の可否を決定し、コンテンツが簡単に外部に洩れそうなコンテンツ保護に対する安全性の弱い機器や、不特定な機器などにコンテンツを送信しないようにする。また、送ったコンテンツが不正に使用されることを防ぐ。
【解決手段】　コンテンツを受信する情報受信側であるコンテンツ取扱装置２を複数の異なる著作権保護レベル及び／又は守秘能力に従って分類し、信頼できる機器にのみ、認証機器１を含む情報送信側がコンテンツの送信を行えるようにする。また本発明は、情報送信側が、コンテンツを受信する情報受信側であるコンテンツ取扱装置を、著作権を有する認証コンテンツデータを用いて認証し、その認証結果に応じてコンテンツの送信の可否を決定し、コンテンツの送信を制御する。
【選択図】　　　図１

認定・付加情報

特許出願の番号　特願２０００－０７９１１２
受付番号　２００００３２０１６２
書類名　特許願
担当官　濱谷　よし子　１６１４
作成日　平成１２年　４月　６日

＜認定情報・付加情報＞
【提出日】　平成12年 2月14日
【特許出願人】
【識別番号】　000004329
【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地
【氏名又は名称】　日本ビクター株式会社
【代理人】　申請人
【識別番号】　100093067
【住所又は居所】　東京都港区芝大門２－４－１　イズミビル３Ｆ
二瓶国際特許事務所
【氏名又は名称】　二瓶　正敬

次頁無

出 願 人 履 歴 情 報

識別番号　〔０００００４３２９〕

１．変更年月日　１９９０年　８月　８日
　［変更理由］　新規登録
　住　所　神奈川県横浜市神奈川区守屋町３丁目１２番地
　氏　名　日本ビクター株式会社